Wachtwoorden in de praktijk

Halt! Wachtwoord?

Wachtwoorden zijn vaak de enige of minstens de laatste beveiliging waarmee je pottenkijkers buiten je persoonlijke gegevens houdt! Wij tonen je hoe je wachtwoorden kiest en gebruikt, beheert én kraakt!

Wat hebben je bankkaarten, Windows, e-mail en ongetwijfeld een hele rist on line services met elkaar gemeen? Juist, je hebt er een code of wachtwoord voor nodig! Ben je begaan met je privacy (of je centjes), dan kies je zoals het hoort voor elke dienst een complex én liefst ook uniek wachtwoord. En dan maar hopen dat je over een paardengeheugen beschikt om al die combinaties van gebruikersnamen en wachtwoorden vast te houden – want ze op een kleefblaadje noteren, neen, daar bezondig jij je niet aan!
Niet verwonderlijk dus dat er allerlei initiatieven opduiken om het de arme gebruiker wat makkelijker te maken. Zo tracht Microsoft met zijn .NET Passport [**www.passport.net**] een systeem in gang te krijgen waarbij één wachtwoord volstaat om je bij tal van on line diensten aan te melden. Best handig, maar dat Microsoft ook hier weer de touwtjes in handen heeft - sámen met je wachtwoord - zorgt voor het nodige wantrouwen... Nog leuker wordt het natuurlijk als je helemáál geen wachtwoord meer nodig hebt, en (een stukje van) je eigen lichaam als wachtwoord kan fungeren, zoals je stem, oog of vingerafdruk. Jammer genoeg bakken deze biometrische experimenten er in de praktijk nog niet zoveel van, en blijken ze nog altijd vrij duur én makkelijk te omzeilen. Toch nog even verder zwoegen met wachtwoorden dus, en daarvoor ben je in dit dossier aan het goede adres...



.NET Passport: één naam, één wachtwoord?

1 Kiezen

Geef toe: het is heel verleidelijk om voor alle diensten en programma's hetzelfde, kort en makkelijk te onthouden wachtwoord te kiezen. Een kleine rekensom maakt echter snel duidelijk dat zo'n exemplaar niet bepaald veilig is. Stel dat je een wachtwoord van vier tekens gebruikt, waarbij je voor je tekenreeks uit alle 26 letters van het alfabet kan putten. Dat komt uit op 26^4 combinaties, of bijna een half miljoen mogelijkheden. Verdubbel je de lengte van je wachtwoord, dan geeft dat dik 200 miljard combinaties (26^8). Dat lijkt indrukwekkend, maar er bestaan wachtwoordkrakers (zie verder) die ettelijke miljoenen combinaties... per seconde kunnen uitproberen! Dat betekent dat zo'n kraakprogramma gemiddeld al na zo'n 2 tot 3 uur met je "onkraakbare" wachtwoord aan de haal gaat! Maak je echter gebruik van een bestaand woord, dan is de kraak vaak nog veel vlugger gepleegd. Veel kraakprogramma's bedienen zich namelijk eerst van uitgebreide woordenlijsten, vooraleer ze andere combinaties uitproberen. Wie zich zelf aan zo'n aanval wil wagen, vindt op [**www.elcomsoft.com/prs.html**] alvast woordenlijsten in meer dan 20 talen (waaronder het Nederlands, met 214.000 ingangen).

De moraal van dit verhaal? Is je wachtwoord de (enige) toegangspoort tot écht belangrijke gegevens, dan zoek je er maar beter een van een zwaarder kaliber. Met een beetje creativiteit hoeft dat trouwens geen hersenbreker te zijn...

Om te beginnen kan je de tekenreeks al verdubbelen, door zowel kleine letters als hoofdletters te gebruiken (in de veronderstelling dat het wachtwoord hoofdlettergevoelig is). En waarom zou je daar niet meteen ook cijfers bij betrekken, zodat je met een wachtwoord van acht tekens al aan $(26+26+10)^8$ mogelijke combinaties zit (bijna 220 biljoen). En je kan er zelfs nog een paar andere tekens – zoals leestekens – bij halen...

Hoe onthoud je nu zo'n wachtwoord? Wat dacht je bijvoorbeeld van het volgende trucje: je neemt een makkelijk te onthouden zin, waarin minstens één getal en een leesteken voorkomt. Vervolgens schrijf je de beginletter van elk woord op, waarbij je een zelfstandig naamwoord een hoofdletter meegeeft. Een voorbeeld: "Beter één vogel in de hand, dan tien in de lucht". Zet je deze spreuk om in een wachtwoord, dan wordt dat: b1VidH,d1oidL. Eventueel kan je de komma nog door een ander teken vervangen (zoals een asterisk *, tilde ˜ of ampersand &), of alle tekens na het achtste weglaten...

Dictionaries and wordlists

New: Now you can get a **Multilingual Wordlists CD** with all the wordlists listed below at $14,95 only, including delivery (anywhere in the world). **Order CD now!**

- English (~3,160,000 words)
- African (~128,000 words)
- Australian (~80,000 words)
- Brazilian portuguese (~129,000 words)
- Croatian (~28,000 words)
- Czech (~290,000 words)
- Danish (~430,000 words)
- Dutch (~214,000 words)
- Finnish (~253,000 words)
- French (~160,000 words)
- German (~1,550,000 words)
- Hungarian (~17,000 words)
- Italian (~288,000 words)
- Japanese (~115,000 words)
- Norwegian (~118,000 words)
- Polish (~110,000 words)
- Portuguese (~32,000 words)
- Russian (~734,000 words)
- Spanish (~370,000 words)
- Swahili (~18,000 words)
- Swedish (~155,000 words)
- Turkish (~25,000 words)

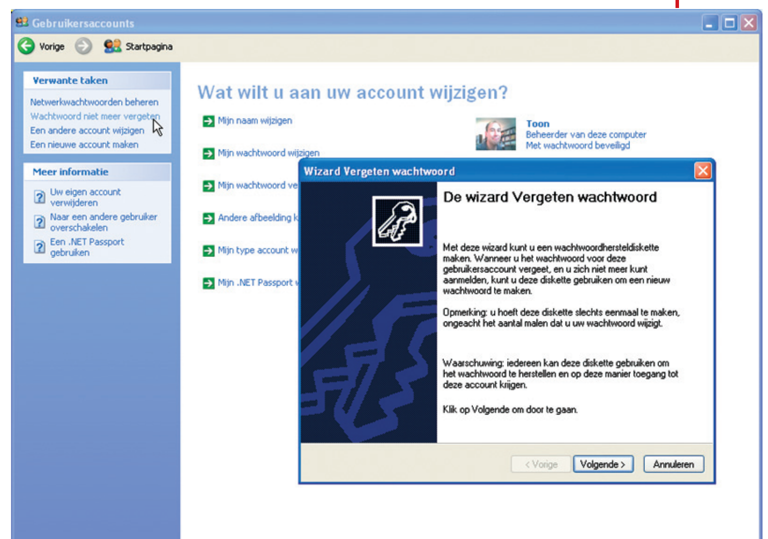
Voer voor bruut geweld...

2 Gebruiken

Zoals gezegd, kan je wachtwoorden inzetten voor tal van programma's en (on line) services. Maar in dit deel tonen wij je hoe je wachtwoorden in enkele bekende toepassingen kan gebruiken. Tegelijk stellen we je ook een paar handige tools voor waarmee je om het even welk bestand kan versleutelen, beschut door een wachtwoord...

XP-accounts

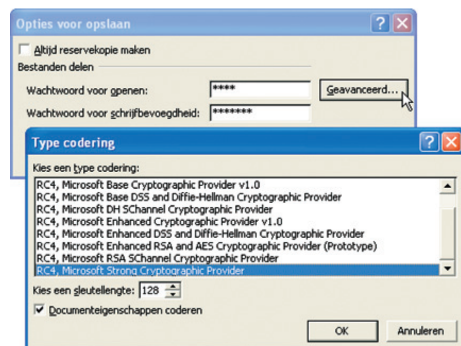
Een doorsnee gezins-pc telt natuurlijk verschillende gebruikers. Hoor jij daar ook bij, dan heb je natuurlijk je eigen gegevens het liefst wat afgeschermd, en dan kan je moeilijk zonder een wachtwoordbeveiligde login (zie ook Clickx 57 en 58). Zo'n wachtwoord koppel je als volgt aan je account: ga naar het CONFIGURATIESCHERM, klik GEBRUIKERSACCOUNTS aan, selecteer je eigen account en kies vervolgens EEN WACHTWOORD INSTELLEN. Je krijgt dan meteen de gelegenheid een geheugensteuntje voor dat wachtwoord in te tikken. Maak het echter ook niet té evident, want dit geheugensteuntje is zichtbaar voor iedereen die op het welkomstscherm op het vraagteken naast je inlognaam klikt. Anderzijds mag je dit wachtwoord ook nooit vergeten, of je loopt het risico jezelf uit te sluiten van je eigen gegevens. Om dat te voorkomen, kan je in Windows XP een speciale wachtwoordherstel-diskette creëren. Hoe ga je tewerk? Roep, zoals hierboven, het venster van je eigen gebruikersaccount op. Selecteer links in het taakvenster WACHTWOORD NIET MEER VERGETEN. Daarmee schud je een wizard wakker die de nodige gegevens naar een (lege) diskette schrijft. Tik je op het welkomstscherm ooit een verkeerd wachtwoord in, dan krijg je automatisch een link naar deze wachtwoordhersteldiskette aangeboden, waarmee je dan een nieuw wachtwoord voor je account kan aanmaken, zonder eerst het oude te moeten intikken. Een veilig plaatsje in je ingebouwde kluis zou niet misstaan voor dit kraakschijfje...



Wachtwoordhersteldiskette: redder in nood?

Microsoft Office

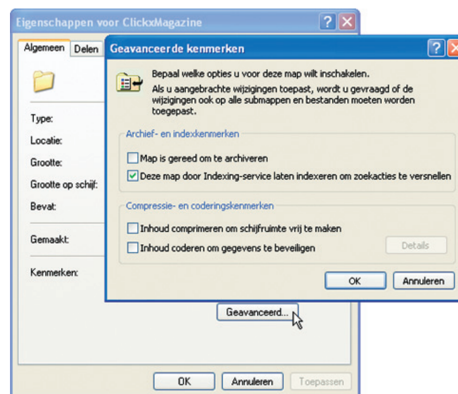
Zowat alle toepassingen van Microsoft's Officesuite laten je toe een wachtwoord aan je documenten te koppelen. Zonder wachtwoord kan je zo'n document dan niet meer openen! We tonen even hoe je een Excel-rekenblad – dat bijvoorbeeld een overzicht van al je gebruikte wachtwoorden bevat? - met een wachtwoord beveiligt (de procedure verloopt bij de andere Office-toepassingen op een gelijkaardige manier).
Is je rekenblad klaar, ga dan naar het menu **BESTAND** en kies **OPSLAAN ALS**. Rechtsboven klik je **EXTRA** aan, en selecteer je **ALGEMENE OPTIES**. Vul nu een wachtwoord in bij **WACHTWOORD VOOR OPENEN**. Druk even op de knop **GEAVANCEERD**: die brengt je naar een venster waar je het versleutelingsalgoritme (zie ook verder) kan instellen. Standaard kiest Microsoft voor een Office 97/2000-compatibel algoritme, maar dat is niet echt de veiligste keuze. Je kan ook opteren voor een RC4-codering (enhanced of strong), met een maximale sleutellengte. En nu dat wachtwoord maar niet vergeten...



Rekenblad beveiligd.

Encryptie

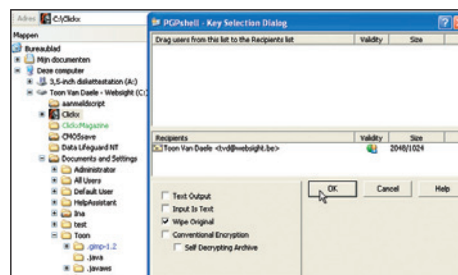
Met de beveiliging van je Office-documenten zit het nu wel snor, maar hoe scherm je willekeurige andere documenten (of zelfs hele mappen) af? Werk je met Windows XP Professional én heb je je schijf(partitie) met het bestandssysteem NTFS geformatteerd, dan zit je gebeiteld. Deze combinatie ondersteunt namelijk encryptie van mappen en bestanden, en het ganse versleutelingsproces verloopt nagenoeg geheel transparant naar de gebruiker toe. Vergeet echter niet dat ook deze beveiliging staat of valt met een wachtwoord, met name dat waarmee je je aanmeldt bij Windows XP. De inhoud van een map versleutelen doe je als volgt. Open de Verkenner, klik met de rechtermuistoets op de bewuste map, en kies **EIGENSCHAPPEN**. Druk nu op de knop **GEAVANCEERD**, en zet een vinkje naast **INHOUD CODEREN OM GEGEVENS TE BEVEILIGEN**. Bevestig je keuze. Alle huidige en nieuwe gegevens in deze map worden voortaan automatisch versleuteld. In de Verkenner krijgt zo'n beveiligde map overigens een apart kleurtje mee (standaard: groen).
Beschik je niet over deze tandem XP Professional–NTFS, niet getreurd: er bestaan nog gratis tools waarmee je ook je ding kan doen...



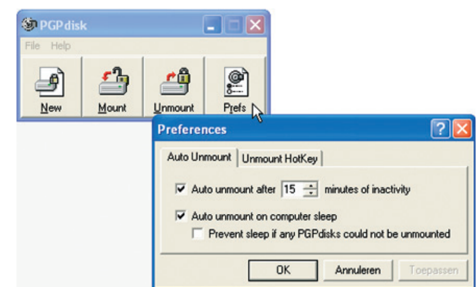
Encryptie: XP Pro én NTFS.

Extra (gratis) tools

Een van de bekendste versleutelingsprogramma's is PGP, wat staat voor pretty good privacy. Het is vooral erg populair om e-mailberichten digitaal te handtekenen en te encrypteren, maar je kan PGP even goed inzetten om willekeurige bestanden op je harde schijf te versleutelen. Voor niet-commercieel gebruik kan je een gratis versie (8.0) van PGP sponzen op [**www.pgpi.org/products/ pgp/versions/freeware**]. Na de installatie moet je dan eerst nog het mee geïnstalleerde programma PGPKeys opstarten. Hiermee maak je de noodzakelijke sleutels aan, beschermd door een 'passphrase' (een wachtwoord, zeg maar). Dat doe je door in het menu **KEYS** de optie **NEW KEY** te selecteren, en vervolgens enkele eenvoudige instructies van een wizard uit te voeren. Is dat achter de rug, dan kan je de Verkenner opstarten, en met de rechtermuistoets het bewuste bestand (of map) aanklikken. Hier kies je dan **PGP**, en vervolgens **ENCRYPT**. Na je bevestiging wordt er een versleutelde versie van het aangeklikte bestand gemaakt. Wil je tegelijk de originele versie kwijt, stip dan de optie **WIPE ORIGINAL** aan. Om het bestand weer te ontsleutelen, selecteer je **DECRYPT** en tik je opnieuw je passphrase in.



Meer privacy met PGP en ABC Chaos.



Virtuele schijven mét wachtwoord.

Orde in de chaos

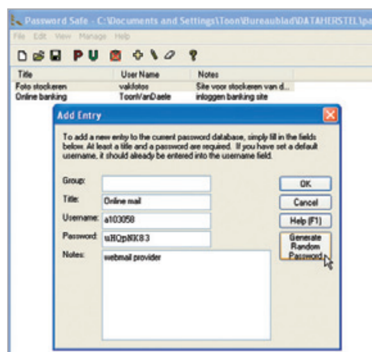
Vergelijkbaar met deze functie van PGP is het gratis programma ABC Chaos [**www.safechaos.com/abc.htm**], dat zich echter minder zwaar aandient. Het principe is eenvoudig: je start het programma op en bladert door je schijf. Bestanden die je wil versleutelen, sleep je naar het middenvenster, waarna je je wachtwoord intikt en op de knop **ENCRYPT** drukt. Ontsleutelen verloopt op nagenoeg dezelfde wijze. Het voordeel van ABC Chaos ten overstaan van PGP is dat je de ganse inhoud van een map in één versleuteld bestand kan stoppen.
Het blijft natuurlijk wel een hele klus om bij elke versleuteling of ontsleuteling van een bestand of map je wachtwoord te moeten intikken. Daarom gooien enkele tools het over een andere boeg: zij creëren een virtuele schijf(partitie) die vanuit je Verkenner bereikbaar is, en je hoeft bij elke sessie slechts één keer je wachtwoord in te geven om die bereikbaar te maken. Gratis tools hiervoor vinden we opnieuw bij PGP, meer bepaald in de vorm van PGPDisk [**www.pgpi.org/products/pgpdisk**]. Jammer genoeg wordt deze tool in de gratis versie van PGP niet meer ondersteund. Je moet je dan maar tevreden stellen met PGPFreeware versie 6.0. PGPDisk bleek vlotjes te werken op ons Windows 98-testsysteem, maar liet onder Windows XP wel een paar steekjes vallen. Hetzelfde geldt voor Scramdisk [**www.scramdisk.clara.net**]: dat kan je nog steeds gratis op de kop tikken voor Windows 9x/ME, maar voor een XP-compatibel product word je doorverwezen naar de commerciële versie DriveCrypt ($ 59,95 – er is wel een gratis demoversie).

3 Beheren

Wie met een rist wachtwoord moet jongleren, zal al vlug de geneugten van een beheertool appreciëren. We hebben dan wel al een voorzichtige aanzet gegeven tot zo'n beheerinstrument in de vorm van een wachtwoordbeveiligd rekenblad (zie hiervoor), maar wat had je gedacht: natuurlijk bestaan ook hier gespecialiseerde - en jawel, zelfs gratis - tools voor!

Kluis

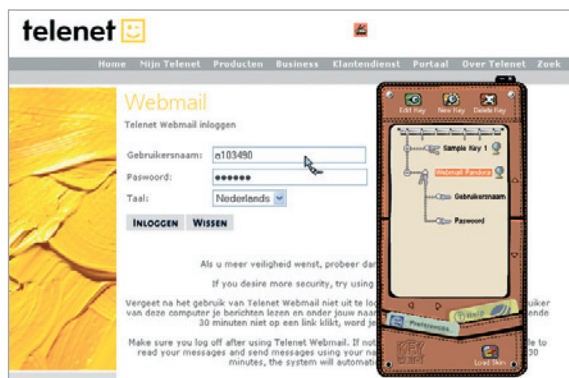
Een ervan is Password Safe [**http://sourceforge.net/projects/passwordsafe**]. De werking is heel simpel: je stockeert gebruikersnamen en wachtwoorden in een databank, die je vervolgens van een "superwachtwoord" voorziet. Eens je de databank hebt geopend, hoef je het gewenste wachtwoord maar aan te klikken en Password Safe sast het door naar het klembord. Van daaruit kan je het dan naar het invoerveld kopiëren. Er is ook al een bètaversie 2 beschikbaar, maar die bleek op ons XP-toestel nog niet helemaal stabiel.



Een kluis voor je wachtwoorden.

Beheertools

Je kan natuurlijk nog méér hulp verwachten van dergelijke beheertools, en de optie **AutoAanvullen**, die je standaard in Internet Explorer vindt, is al een eerste aanzet daartoe. Hiermee kan je je browser zo instellen dat hij gebruikersnamen en wachtwoorden voor webformulieren voor jou versleuteld opslaat op je harde schijf, en die automatisch invult als je dat formulier nog een keer oproept: niet echt veilig natuurlijk, als je met meer personen op één pc werkt... Deze optie vind je in het menu **Extra**, bij **Internet-opties**. Hier open je het tabblad **Inhoud** en druk je op de knop **AutoAanvullen**.
Gratis tools als RoboForm [**www.roboform.com**] en KeyWallet [**www.keywallet.com**] hebben dit spoor opgenomen en verder ontwikkeld. Ook Gator's eWallet [**www.claria.com/products**] is zo'n beheertool, maar hier huist jammer genoeg ook spyware in. Al deze tools kunnen niet alleen je wachtwoorden en gebruikersnamen onthouden, ze kunnen ook webformulieren grotendeels volautomatisch invullen. Het voordeel van deze tools is bovendien dat ze niet gebonden zijn aan een bepaald browsertype (hoewel RoboForm zich als een vis in het water voelt bij Internet Explorer).



Wachtwoorden: in de pocket!

4 Kraken

Jou zullen ze niet liggen hebben: je hebt al je wachtwoorden met zorg gekozen én een beheertool houdt ze allemaal netjes bij. Maar wat als die er onverwachts de brui aan geeft, en je geheugen wel een gatenkaas lijkt? In dat geval kan je maar beter hopen op een achterpoortje ...

Voor het grijpen

Gelukkig (nu ja...) blijken sommige wachtwoorden wel erg makkelijk te achterhalen! Dat ligt dan niet zozeer aan de keuze van dat wachtwoord, maar wel aan de manier waarop het programma of de service met je wachtwoord omspringt. Een voorbeeld. Stel dat je het wachtwoord om je aan te melden bij de mailserver niet meer kent. Dan kan je dat wellicht nog bij je provider te weten komen, maar het kan nog stukken makkelijker. Je hoeft er enkel het gratis tooltje SnadBoy's Revelation [**www.snadboy.com**] voor te downloaden. Zodra je het programma hebt opgestart, sleep je een icoontje over het wachtwoordveld, en ziedaar: de tool vertelt je meteen welke tekens er achter al die asteriskjes schuilgaan!

Vergeet ook niet dat heel wat wachtwoorden onversleuteld – over je netwerk? – het net opgaan. Het volstaat een zogenaamde netwerksniffer (zoals het gratis Ethereal, op [**www.ethereal.com**]) op te starten die je uitgaande verkeer monitort, en voor je het weet, heeft die je e-mail- of ftp-wachtwoord te pakken.

Kraaktools

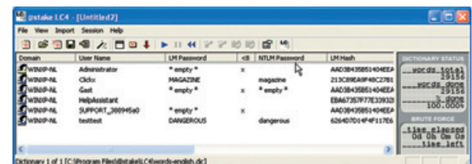
Verwacht nu niet dat je Windows- of Office-wachtwoorden even makkelijk te achterhalen vallen: daar komt heus wel wat zwaarder materiaal bij kijken. Kraaktools dus... Hoe werken die eigenlijk? Daarvoor moet je eerst weten hoe een wachtwoord gewoonlijk wordt opgeslagen. Elk deftig programma zorgt er natuurlijk voor dat zo'n wachtwoord niet zomaar op je schijf gedropt wordt. Daar wordt normaal eerst een versleutelingsalgoritme op toegepast, met jouw wachtwoord als invoer. Het resultaat van deze berekening noemen we een 'hash', en die wordt op schijf opgeslagen. Krijgt iemand deze hash te pakken, dan hoef je nog niet te panikeren: normaal kan die vanuit zo'n hash nooit je wachtwoord afleiden! Hoe gaan kraaktools gewoonlijk dan wél tewerk? Heel eenvoudig: ze vuren miljoenen mogelijke woordcombinaties af waarop ze het versleutelingsalgoritme toepassen, en de resulterende hash vergelijken ze met jouw hash. Blijken beide exemplaren overeen te komen, dan is meteen ook je wachtwoord gevonden!

Goede kraaktools die ook nog eens gratis zijn, liggen op het internet niet zo dik bezaaid. Bekend is alvast LOphtCrack (onder meer te vinden op [**www.evadenet.com/downloads/lophtcrack.shtml**]), dat het vooral gemunt heeft op inlogwachtwoorden voor bepaalde Windows-versies, en dat eventueel gebruik kan maken van de tools Samdump en PWdump om je wachtwoordhashes te bemachtigen.

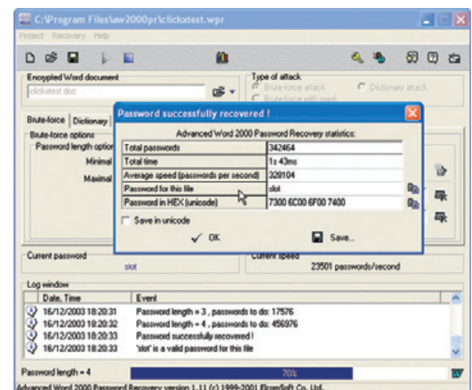
De meest recente versie van deze kraker zit intussen ook al in een commercieel jasje: @stake LC4 ([**www.atstake.com/products/ lc**], waar je terecht kan voor een beperkte demo).

Maar wat als je bijvoorbeeld een wachtwoord van een Office-document vergeten bent, of van een gearchiveerd bestand (zoals zip-bestanden)? Geen nood, ook hiervoor vind je de nodige tools. Op [**www.lostpassword.com**] bijvoorbeeld tref je kraakmodules aan voor de meest uiteenlopende toepassingen. De gratis demoversies kan je jammer genoeg enkel uitproberen op wachtwoorden van maximaal twee tekens. Ook ElcomSoft [**www.elcomsoft.com/prs.html**] heeft zich op deze materie toegelegd, en op hun stek kan je eveneens terecht voor demoversies.

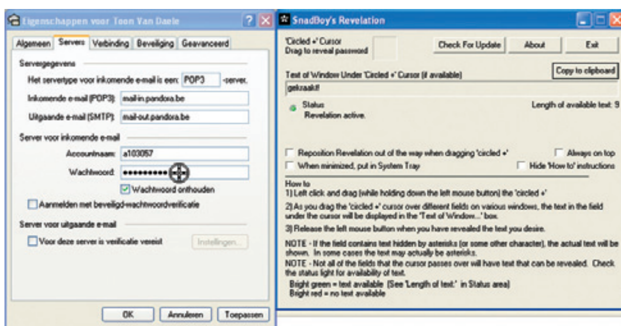
— Toon Van Daele —

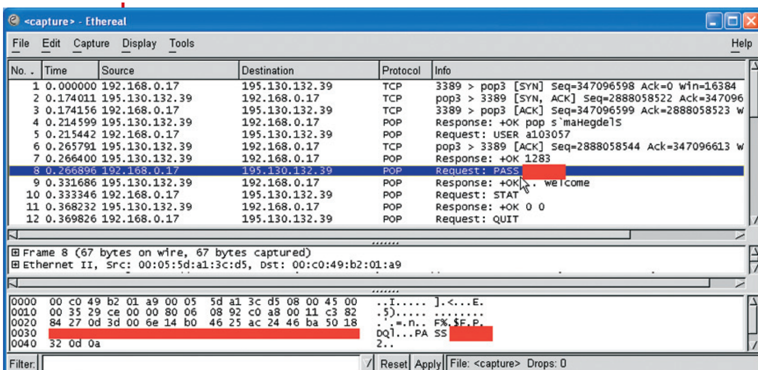






Wachtwoorden: gekraakt in 2 seconden.





Wachtwoorden te grabbel met Revelation en Ethereal.

BESLUIT

Wachtwoordtools zijn er in allerlei maten en gewichten. Het gaat van programma's om bestanden met zo'n wachtwoord te beveiligen, over tools om je wachtwoorden te helpen beheren tot... heuse kraakprogramma's waarmee je (vergeten?) wachtwoorden weer tevoorschijn kan halen! Maak je je eigen exemplaren toch liever wat kraakbestendiger, dan is het alvast géén goed idee om inspiratie te zoeken in het woordenboek...